

Patent Claims

1. Method for automatically identifying an access right to protected areas in a first network using a unique connection identifier of a second network, in particular in the interconnection of networks that constitutes the internet, with the following procedural steps:
 - dynamic or static assignment of a unique identifier of the first network for a terminal, during or prior to the latter's connection to the first network;
 - storage of a combination of at least the unique connection identifier of the second network and the unique identifier of the first network in an authentication unit;
 - requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area;
 - checking whether an access right for the protected area exists for the unique connection identifier of the second network.
2. Method in accordance with claim 1, characterised in that the combination stored in the current authentication unit contains further data in addition.
3. Method in accordance with claim 2, characterised in that the additional data has at least one of the following: the dial-in number into the first network, a user name (login) and a password.
4. Method in accordance with any of the previous claims, characterised in that the authentication unit is only run temporarily.
5. Method in accordance with claim 4, characterised in that the combination of data is deleted from the authentication unit as soon as the terminal ends its connection with one of the two networks.

6. Method in accordance with any of the previous claims, characterised in that the unique identifier of the second network is a call-up number.
7. Method in accordance with any of the previous claims, characterised in that the protected area includes the provision of an online individual connection identification.
8. Method in accordance with claim 7, characterised in that a individual connection identification takes place automatically for the unique connection identifier of the second network.
9. Method in accordance with claim 7, characterised in that, before release of a individual connection identification, a further entry on the terminal is necessary in addition.
10. Method in accordance with claim 9, characterised in that the further entry includes the entry of an invoice number and/or a customer number and/or a PIN.
11. Method in accordance with any of the previous claims, characterised in that only authorised services have access to the authentication unit.
12. Method in accordance with any of the previous claims, characterised in that the protected area includes at least one of the following services: provision of contents, electronic trade (e-commerce), payment or settlement services and authorised services.
13. Method in accordance with claim 12, characterised in that with a payment service, the costs arising are automatically invoiced by means of the unique connection identifier of the second network.

14. Method in accordance with any of the previous claims, characterised in that further data are automatically called up from the terminal and/or further procedural steps are initiated in the protected area using the unique connection identifier of the second network.
15. Method in accordance with any of the previous claims, characterised in that further personalisation of the terminal takes place by entering a PIN.
16. Method for providing data for automatic identification of access rights to protected areas in networks, in particular in the interconnection of networks that constitutes the internet, with the following procedural steps:
 - provision of at least one unique identifier respectively from at least two different networks while a connection to both networks exists;
 - storage of a combination of the different identifiers in an authentication unit;
 - issue and/or authentication of one of the unique identifiers when a corresponding enquiry is made regarding the other unique identifiers;
 - deletion of the data from the authentication unit as soon as a connection with at least one of the two networks has ended.
17. Method in accordance with claim 16, characterised in that at least one of the identifiers is an IP number and/or a unique connection identifier of a terminal.
18. Method in accordance with claim 16 or 17, characterised in that it is checked whether the enquiry originates from an authorised place or from an authorised service.
19. Method in accordance with any of the claims 16 to 18, characterised in that the combination stored in the current authentication unit contains further information in addition.

BEST AVAILABLE COPY

20. Method in accordance with claim 19, characterised in that the additional data have at least one of the following: a dial-in number into one of the networks, a user name (login) and a password.
21. Method in accordance with any of the claims 16 to 20, characterised in that a call-up number block or a target number block is identified by means of the authentication unit.